CLAIMS

What is claimed is:

1.   A method for blocking dereferencing elements in a message, the method

comprising:

accepting a source file for the message;

identifying one or more elements within the message source file, wherein the

elements specify references to sources of content to be dereferenced upon

rendering of the message;

rewriting the references to the sources of content of the elements identified in the

message source;

passing the message source to a message display output; and

rendering the message in the message display.

2.   The method of claim 1 further comprising specifying a security policy setting,

wherein the rewriting of the references to the sources of content is in accordance

with the security policy setting.

3.   The method of claim 1 wherein the rewriting of the references to the sources of

content comprises replacing the reference to the source of content with an empty

string.

4.   The method of claim 1 wherein the rewriting of the references to the sources of content comprises replacing the reference to the source of content with a reference to an alternate source file.

5.   The method of claim 4 wherein the alternate source file is a transparent image file.

6.   The method of claim 1 wherein the message source file is a Hypertext Mark-up Language (HTML) document.

7.   The method of claim 1 wherein the message display is an HTML rendering display.

8.   A computer-readable medium containing instructions for performing a method for blocking dereferencing elements in a message, the method comprising:

accepting a source file for the message;

identifying one or more elements within the message source file, wherein the elements specify references to sources of content to be dereferenced upon rendering of the message;

rewriting the references to the sources of content of the elements identified in the message source;

passing the message source to a message display output; and

rendering the message in the message display.

9.   A method for removing referring source information in a hyperlinked document,

the method comprising:

accepting a source file for the document;

identifying one or more elements within the message source file, wherein the

elements specify references to hyperlinks;

rewriting the references to the hyperlinks identified in the message source to be

prepended with a reference to a redirect file;

passing the message source to a message display output; and

rendering the message in the message display.

10.   The method of claim 9 further comprising specifying a security policy setting,

wherein the rewriting of the references to the hyperlinks is in accordance with the

security policy setting.

11.   The method of claim 9 wherein the message source file is an HTML document.

12.   The method of claim 9 wherein the message display is an HTML rendering

display.

13.   A computer-readable medium containing instructions for performing a method for

removing referring source information in a hyperlinked document, the method

comprising:

accepting a source file for the document;

identifying one or more elements within the message source file, wherein the elements specify references to hyperlinks;

rewriting the references to the hyperlinks identified in the message source to be prepended with a reference to a redirect file;

passing the message source to a message display output; and

rendering the message in the message display.

14. A method for blocking dereferencing elements in a message, the method comprising:

accepting a source file for the message;

rendering the file in a first message display output;

grouping one or more elements within the rendered message into security level groups;

rewriting the elements to be processed through a protocol handler;

passing the message source to a second message display output; and

rendering the message in the second message display.

15. The method of claim 14 further comprising specifying a security policy setting, wherein the processing of the elements by the protocol handler is in accordance with the security policy setting.

16.   The method of claim 15 wherein the processing of the elements by the protocol handler comprises redirecting to an original target destination.

17.   The method of claim 15 wherein the processing of the elements by the protocol handler comprises returning information indicating that a target destination is not available.

18.   The method of claim 15 wherein the processing of the elements by the protocol handler comprises redirecting to an alternate source file.

19.   The method of claim 18 wherein the alternate source file is a transparent image file.

20.   The method of claim 14 wherein the message source file is an HTML document.

21.   The method of claim 14 wherein the first and second message displays are HTML rendering displays.

22.   A computer-readable medium containing instructions for performing a method for blocking dereferencing elements in a message, the method comprising:

accepting a source file for the message;

rendering the file in a first message display output;

grouping one or more elements within the rendered message into security level groups;

rewriting the elements to be processed through a protocol handler;

passing the message source to a second message display output; and

rendering the message in the second message display.

23. A method for blocking dereferencing elements in a message, the method comprising:

accepting a source file for the message;

rendering the file in a first message display output;

grouping one or more elements within the rendered message into security level groups;

rewriting the elements to be processed through a protocol handler;

passing the message source to a second message display output;

rendering the message in the second message display;

combining a base Uniform Resource Locator (URL) and a relative URL into a full URL; and

passing the full URL to be processed to a protocol handler.

24. The method of claim 23 further comprising specifying a security policy setting, wherein the processing of the elements by the protocol handler is in accordance with the security policy setting.

25. The method of claim 24 wherein the processing of the elements by the protocol handler comprises redirecting to an original target destination.

26. The method of claim 24 wherein the processing of the elements by the protocol handler comprises returning information indicating that a target destination is not available.

27. The method of claim 24 wherein the processing of the elements by the protocol handler comprises redirecting to an alternate source file.

28. The method of claim 27 wherein the alternate source file is a transparent image file.

29. The method of claim 23 wherein the message source file is an HTML document.

30. The method of claim 23 wherein the first and second message displays are HTML rendering displays.

31. A computer-readable medium containing instructions for performing a method for blocking dereferencing elements in a message, the method comprising:

accepting a source file for the message;

rendering the file in a first message display output;

grouping one or more elements within the rendered message into security level groups;

rewriting the elements to be processed through a protocol handler;

passing the message source to a second message display output;

rendering the message in the second message display;

combining a base URL and a relative URL into a full URL; and

passing the full URL to be processed to the protocol handler.